



FortiMail™

Comprehensive Email Security



Proven Security

FortiMail appliances and virtual appliances are proven, powerful email security platforms for any size organization — from small businesses to carriers, service providers, and large enterprises. Purpose-built for the most demanding messaging systems, FortiMail appliances employ Fortinet's years of experience in protecting networks against spam, malware, and other message-borne threats.

Intelligent Protection

FortiMail prevents your email systems from becoming threat delivery systems. Its inbound filtering engine blocks spam and malware before it can clog your network and affect users. Its outbound inspection technology prevents other antispam gateways from blacklisting your users by blocking outbound spam and malware, including mobile traffic.

Enforce secure content delivery with FortiMail Identity-Based Encryption (IBE), S/MIME, or TLS email encryption options. Prevent accidental and intentional loss of confidential data using predefined HIPAA, GLBA, SOX or customized dictionaries.

Key Features & Benefits

Deploy appliances or virtual appliances in Transparent, Gateway, or Server modes	FortiMail can be deployed in gateway, transparent mode and uniquely as a fully featured mail server. It can be deployed as CPE or in the cloud and in hardware or VM form factors. FortiMail is flexible enough to cater for every customer requirement.
Apply Identity-Based Encryption in both push and pull methods	Ensures secure delivery of confidential or regulated content. Extremely easy to deploy — no additional hardware or software to install, no user provisioning, no pre-enrollment for recipient.
Data Loss Prevention and Compliance	Detect accidental or intentional loss of confidential or regulated data. Achieve PCI-DSS, HIPAA, GLBA or SOX compliance by blocking messages containing defined data patterns, or creating policies to enforce encryption of certain emails.
Identify and Block Spamming Endpoints	Prevent blacklisting of legitimate subscribers by identifying and blocking endpoints sending spam, including Smart phones. Ideal for Carriers and Service Providers.
No per-user or per-mailbox pricing	Complete, multi-layered antivirus, antispam, antispysware and antiphishing protection for an unlimited number of users. Greatly reduces TCO.

Comprehensive Email Security

- Inspect over 28 million messages per hour in a single appliance
- Unmatched deployment flexibility
- Apply Identity-Based Encryption in both push and pull methods
- Data Leak Prevention, and Policy-Based Encryption and Archiving enable compliance with SOX, GLBA, HIPAA, PCI DSS
- Enforce email and security policies at a granular level
- Receive real-time security updates from FortiGuard® Services
- Industry leading price/performance
- Flexible deployment modes and architectures support the widest range of organizations
- Multi-layer threat detection delivers highest level of user protection
- Scalable solution delivers long term investment protection



FortiCare

Worldwide 24x7 Support
support.fortinet.com



FortiGuard

Threat Research & Response
www.fortiguards.com

High Performance and Unmatched Flexibility

FortiMail appliances provide high-performance email routing and security by utilizing multiple high-accuracy antispam filters. When coupled with industry leading real-time antivirus and antispymware protection from FortiGuard Services, FortiMail provides you with extremely fast and accurate email security

that won't affect end users or delay their communications. FortiMail can be deployed in the cloud or on premises and gateway, inline and server modes in a range of appliance or virtual machine form factors. This flexibility allows you to deploy FortiMail in the mode that best suits your environment.

FEATURES

System

- Transparent, Gateway and Server Mode Deployment Options
- Flexible Interface Configuration Including VLAN and Redundant Interface Support
- Inbound and Outbound Inspection
- Multiple Email Domains with Domain Level Customization
- IPv6 and IPv4 Address Support
- Virtual Hosting using Source and/or Destination IP Address Pools
- Policy-Based Mail Archiving with Remote Storage Options
- SMTP Authentication Support via LDAP, RADIUS, POP3 and IMAP
- LDAP-Based Email Routing
- Per User Inspection using LDAP Attributes on a Per Policy (Domain) Basis
- Comprehensive Webmail Interface for Server Mode Deployments and Quarantine Management
- Mail Queue Management
- Multiple Language Support for Webmail and Admin Interface
- Email RFC Compliance
- Maintains Local Sender Reputation List Based on:
 - Sender Policy Framework (SPF)
 - Domain Keys Identified Mail (DKIM)

Management, Logging, and Reporting

- QuickStart Setup Wizard
- Basic / Advanced Management Modes
- Role-Based Administration Accounts Per Domain
- Comprehensive activity and incident logging and reporting
- Configuration Change and Management Event Logging
- Built-in Reporting module
- FortiManager and FortiAnalyzer Support for Central Management and Reporting
- Centralised Quarantine for large scale deployments
- SNMP Support using Standard and Private MIB with Threshold-Based Traps
- External or Local Storage Server Support, including iSCSI devices
- External Syslog support

High Availability (HA)

- Supported in all Modes
- Active-Passive Mode
- Configuration Synchronization Mode (Configuration Master and Slave Mode)
- Quarantine and Mail Queue Synchronization
- Device Failure Detection and Notification
- Link Status, Failover and Redundant Interface Support

Antispam Profile

- FortiGuard Antispam Service
 - Global Sender Reputation
 - Spam and phishing URLs and email addresses
 - Spam Object checksums
 - Dynamic Heuristic Rules
- Greylisting for IPv4, IPv6 addresses and email accounts
- Local Sender Reputation (IPv4, IPv6 and End Point ID based)
- Deep Email Header Inspection
- Flexible Action and Notification Profiles
- Third party Spam URI and Real-Time Blacklists (SURBL/RBL)
- Full category FortiGuard URL Filtering
- Quarantining, tagging and end user reporting
- PDF Scanning and Image Analysis
- Black/White Lists at Global, Domain, and User levels
- Bayesian Statistic Filtering
- Newsletter detection

Antivirus

- FortiGuard Antivirus Service
- Quarantine, Repackage, Replace, and Monitor Actions
- Nested Archive Scanning
- Malware Detection

Content-Based Protection

- Dictionary-based filtering in inbound or outbound direction
- Predefined HIPAA, GLBA and SOX dictionaries
- Filter by Attachment File Type
- Banned Word Filtering

Denial-of-Service Protection

- Inbound and Outbound Message Rate Limiting
- Recipient Address Attack
- Reverse DNS Check (Anti-Spoofing)
- Forged Sender Address

Encryption

- Identity-based Encryption for Push/Pull Delivery of Encrypted Messages
- S/MIME Support for Gateway-to-Gateway Encryption
- Support for strong-crypto protocols including HTTPS, SMTPS, SSH, IMAPS and POP3S

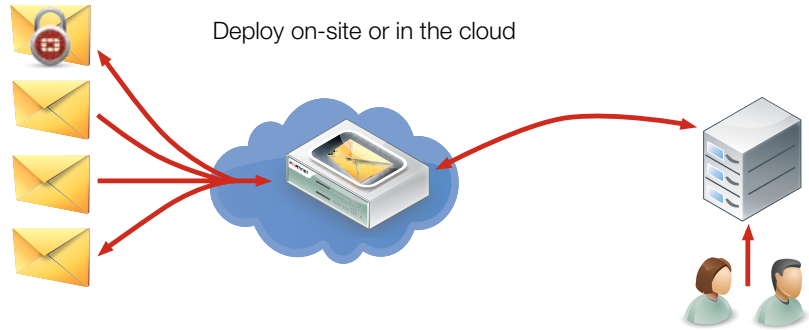
Server Mode Specific Features

- SMTP, IMAP, and POP3 Email Services
- SMTP over SSL Support
- Disk Quota Policy Support for User Accounts
- Secure WebMail Client Access
- User, Group and Alias List Support
- Local Account and LDAP Authentication
- WebMail Calendar
- Email Auto Reply and Forwarding Preference
- Address Book Synchronize with LDAP

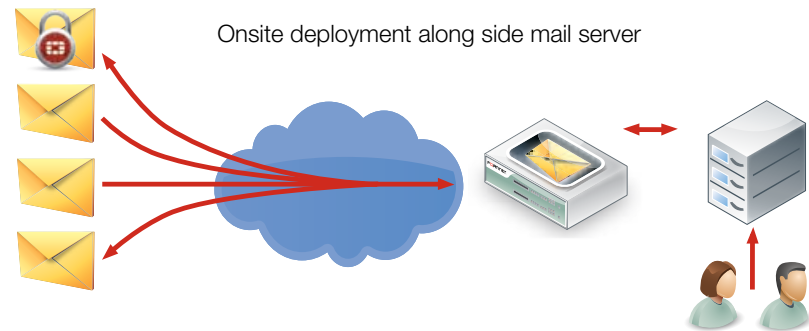
FortiMail Deployment Options

Choose from three modes of deployment — Transparent, Gateway, or Server mode – to meet your specific email security requirements, while minimizing infrastructure changes and service disruptions:

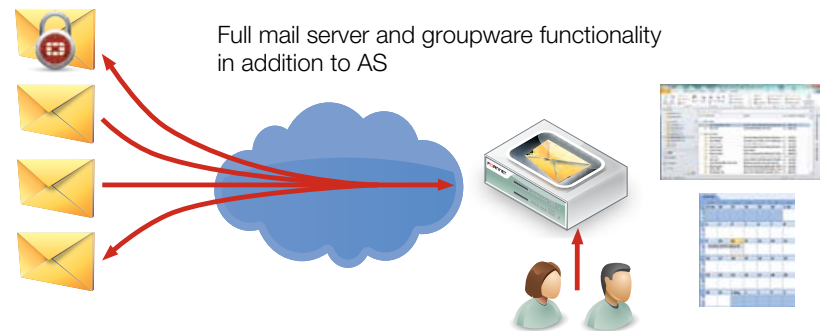
Gateway Mode: Provides inbound and outbound proxy mail transfer agent (MTA) services for existing email gateways. A simple DNS MX record change redirects email to FortiMail for antispam and antivirus scanning. The FortiMail device receives messages, scans for viruses and spam, then relays email to its destination email server for delivery.



Transparent Mode: Each network interface includes a proxy that receives and relays email. Each proxy can intercept SMTP sessions even though the destination IP address is not the FortiMail appliance. FortiMail scans for viruses and spam, then transmits email to the destination email server for delivery. This eliminates the need to change the DNS MX record, or to change the existing email server network configuration.

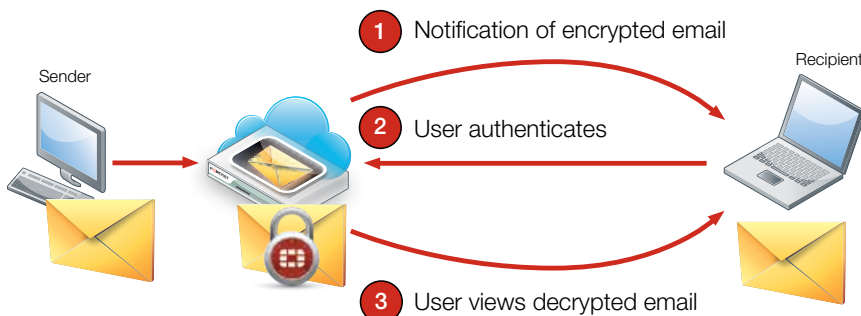


Server Mode: The FortiMail device acts as a stand-alone messaging server with full SMTP email server functionality, including flexible support for secure POP3, IMAP and WebMail access. FortiMail scans email for viruses and spam before delivery. As in Server mode, external MTAs connect to FortiMail, allowing it to function as a protected server.



Identity-Based Encryption (IBE)

IBE allows FortiMail to deliver confidential and regulated email securely — without requiring additional hardware, software user provisioning, or extra license fees. Use IBE to eliminate paper-based communications and reduce costs.



Policy-Based Encryption: Automatically encrypt messages for compliance, based on content or recipient.

Push or Pull Mode: Use Push, Pull, or a combination of modes to meet your requirements.

Easy to Deploy, Use, and Manage: Deploy IBE in any mode, including Transparent mode, without user provisioning or additional hardware or software.

SPECIFICATIONS

	FORTIMAIL-200D	FORTIMAIL-400C	FORTIMAIL-1000D	FORTIMAIL-3000C	FORTIMAIL-3000D	FORTIMAIL-5002B
Hardware Specifications						
10/100/1000 Interfaces (Copper, RJ-45)	4	4	6	4	4	3
SFP Gigabit Ethernet Interface	0	0	2	2	2	0
Internal Backplane Base / Fabric Channel Interfaces	0	0	0	0	0	2/ 2
Redundant Hot Swappable Power Supplies	No	No	Yes	Yes	Yes	N/A
Storage	1x 1 TB	2x 1 TB	2x 2 TB (2x 2 TB Optional)	2x 1 TB (4x 1 TB Optional)	2x 2 TB (6x 2 TB Optional)	1x 146 GB HDD (RTM Module included)
RAID Storage Management	No	Software: 0, 1	Hardware: 1, 5, 10, 50, Hot Spare (Based on Drive Count)	Hardware: 1, 5, 10, 50, Hot Spare (Based on Drive Count)	Hardware: 1, 5, 10, 50, Hot Spare (Based on Drive Count)	No
Form Factor	Rack Mount Appliance	Rack Mount Appliance	Rack Mount Appliance	Rack Mount Appliance	Rack Mount Appliance	ATCA Chassis Blade
System Specifications						
Email domains	50	500	5,000	5,000	5,000	10,000
Recipient based policies (per Domain / per System) – incoming or outgoing	60 / 300	600 / 3000	1,500 / 7,500	1,500 / 7,500	1,500 / 7,500	1,500 / 7,500
Server Mode Mailboxes	200	1,000	3,000	3,000	3,000	3,000
Antispam, Antivirus, Authentication, and Content Profiles (per Domain / per System)	50 / 60	50 / 200	50 / 600	50 / 600	50 / 600	50 / 600
Unlimited User Licenses				Yes		
Performance (Messages/Hour) [Without queuing based on 3 KB message size]						
Email Routing	200,000	400,000	1.7 Million	2.0 Million	2.3 Million	2.3 Million
FortiGuard Antispam	180,000	350,000	1.4 Million	1.8 Million	2.2 Million	2.2 Million
FortiGuard Antispam + Antivirus	175,000	320,000	1.3 Million	1.6 Million	2.0 Million	2.0 Million
Dimensions						
Height x Width x Length (in)	1.75 x 17.05 x 13.86	1.70 x 17.10 x 14.30	3.50 x 17.24 x 14.49	3.46 x 17.40 x 29.00	3.50 x 20.00 x 29.70	1.18 x 14.00 x 12.20
Height x Width x Length (mm)	45 x 433 x 352	44 x 435 x 364	88 x 438 x 368	88 x 442 x 737	88 x 442 x 737	30 x 355 x 310
Weight	13.4 lbs (6.1 kg)	16.1 lbs (7.3 kg)	57.5 lbs (26.1 kg)	50.0 lbs (22.7 kg)	71.5 lbs (32.5 kg)	7.4 lbs (3.4 kg)
Environment						
Power Source			100–240 VAC, 50–60 Hz			-40.5 V (DC) to -57 V (DC)
Maximum Power Required	1.00A/110V, 0.50A/220V	4.00A/110V, 2.00A/220V	3.50A/110V, 1.75A/220V	7.0A/110V, 3.5A/220V	10.0A/110V, 5.0A/220V	9.4A/110V, 4.7A/220V
Power Consumption (AVG)	60 W	100 W	115 W	200 W	340 W	148 W
Heat Dissipation	205 BTU/h	342 BTU/h	471 BTU/h	683 BTU/h	1160 BTU/h	505 BTU/h
Humidity	5–95% non-condensing	10–90% non-condensing	5–95% non-condensing	5–95% non-condensing	20–90% non-condensing	5–93% non-condensing
Operating Temperature	32–104°F (0 – 40°C)	32–104°F (0–40°C)	32–104°F (0–40°C)	50–95°F (10–35°C)	50–95°F (10–35°C)	32–131°F (0–55°C)
Storage Temperature	-13–158°F (-25–70°C)	-4–158°F (-20–70°C)	-13–158°F (-25–70°C)	-40–149°F (-40–65°C)	-40–149°F (-40–65°C)	-40–158°F (-40–70°C)
Compliance						
	FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB			FCC Part 15 Class A, C-Tick, VCCI, CE, BSMI, KC, UL/cUL, CB, GOST		FCC Part 15 Class A, CE, UL/cUL, CB
						FCC 47 CFR Part 15, Class A, CE (EN55022/ EN55024/EN300386), CE (EN60950-2001), UL60950-1/CSA22.2
Certifications						
	VBSpam and VB100 rated	VBSpam and VB100 rated, Common Criteria EAL 2+, FIPS 140-2 Validation	VBSpam and VB100 rated	VBSpam and VB100 rated, Common Criteria EAL 2+, FIPS 140-2 Validation	VBSpam and VB100 rated	VBSpam and VB100 rated



FortiMail-200D



FortiMail-400C



FortiMail-1000D



FortiMail-3000C



FortiMail-3000D




FortiMail-5002B

SPECIFICATIONS

VIRTUAL APPLIANCES	VM01	VM02	VM04	VM08
Technical Specifications				
Hypervisors Supported	VMware ESXi / ESX 3.5 / 4.0 / 4.1 / 5.0 / 5.1			
Virtual Machine Form Factor	Open Virtualization Format (OVF)			
Maximum Virtual CPUs Supported	1	2	4	8
Virtual NICs Required (Min/Max)	1 / 4	1 / 4	1 / 4	1 / 4
Virtual Machine Storage Required (Min/Max)	50 GB / 1 TB	50 GB / 2 TB	50 GB / 4 TB	50 GB / 8 TB
Virtual Machine Memory Required (Min/Max)	1 GB / 2 GB	1 GB / 4 GB	1 GB / 8 GB	1 GB / 16 GB
System Performance				
* Email Routing	90,000	265,000	1.32 Million	1.76 Million
* FortiGuard Antispam	85,000	234,000	1.14 Million	1.58 Million
* FortiGuard Antispam + Antivirus	77,000	185,000	1.05 Million	1.40 Million
System Specifications				
Email Domains	50	500	5,000	5,000
Recipient-Based Policies (Domain/System)	60 /300	600 / 3,000	1,500 / 7,500	1,500 / 7,500
Server Mode Mailboxes	200	1,000	3,000	3,000
Profiles (Domain/System)	50 / 60	50 / 200	50 / 600	50 / 600
Unlimited User License	Yes			

* Hardware dependent

	GLOBAL HEADQUARTERS	EMEA SALES OFFICE	APAC SALES OFFICE	LATIN AMERICA SALES OFFICE
	Fortinet Inc. 1090 Kifer Road Sunnyvale, CA 94086 United States Tel: +1.408.235.7700 Fax: +1.408.235.7737	120 rue Albert Caquot 06560, Sophia Antipolis, France Tel: +33.4.8987.0510 Fax: +33.4.8987.0501	300 Beach Road #20-01 The Concourse Singapore 199555 Tel: +65.6513.3730 Fax: +65.6223.6784	Prol. Paseo de la Reforma 115 Int. 702 Col. Lomas de Santa Fe, C.P. 01219 Del. Alvaro Obregón México D.F. Tel: 011-52-(55) 5524-8480

Copyright© 2013 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, and FortiGuard®, are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance metrics contained herein were attained in internal lab tests under ideal conditions, and performance may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to the performance metrics herein. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any guarantees. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable. Certain Fortinet products are licensed under U.S. Patent No. 5,623,600.